# The Information Commissioner's Office response to IMPRESS's consultation on the IMPRESS Standards Code.

## About the ICO

The Information Commissioner has responsibility in the UK for promoting and enforcing the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA 2018), the Freedom of Information Act 2000 (FOIA), the Re-Use of Public Sector Information Regulations 2015 (RPSI), the Environmental Information Regulations 2004 (EIR) and the Privacy and Electronic Communications Regulations 2003 (PECR), amongst others. The Commissioner is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

## ICO response

Thank you for the opportunity to respond to your consultation on the IMPRESS Standards Code ("the Standards Code").

We have responded to your request for evidence in relation to parts 4, 5 and 6 only as these seemed most relevant to our role as regulator of the data protection legislation.

### 4. Accuracy

Whether the Code embodies best practice around signalling news content, the use and placement of corrections, and clarifications (for example, practices around labelling, positioning and transparency), the conflation of fact and opinion and the use of click-bait headlines. Whether the Code embodies best practice for testing veracity, verifiability and robust news gathering, particularly online.

Accuracy is one of the key data protection principles at the heart of data protection law. The UK GDPR says that personal data must be:

"Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay".

Please see our Guide to UK GDPR – Accuracy for more information about this principle.

In practice, the accuracy principle means that organisations must:

- take reasonable steps to ensure the accuracy of personal data
- ensure that the source and status of personal data is clear
- carefully consider any challenges to the accuracy of the information; and
- consider whether it is necessary to periodically update the information.

Those processing personal data for the purposes of journalism must comply with the above data protection principle unless they consider that the special purposes exemption applies under the Data Protection Act 2018 (DPA 2018). This exemption protects freedom of expression in journalism, academic activities, art and literature. For more information, please see our guide for the media. Please note that we are currently working on a journalism code of practice to replace this guidance in line with our statutory obligation.

To rely on the special purposes exemption, those processing personal information for the purposes of journalism must:

1) act with a view to publication;

2) reasonably believe publication is in the public interest; and

3) reasonably believe that compliance with a relevant data protection provision would be incompatible with journalism.

If the special purpose exemption is not being relied upon and an individual submits a request to exercise their rights under data protection law, the organisation should take appropriate steps to ensure compliance. For more information about these rights, please see our Guide to UK GDPR – Individual rights.

The Standards Code states that publishers must take all reasonable steps to ensure accuracy but it does not refer to the relevant rights that individuals have under data protection law specifically (the right to erasure, the right to rectification and the right to restriction). These are important rights designed to give people more control over their personal data when they have concerns about inaccuracy. You may wish to consider referring to these rights in the Standards Code and/or the other points bulleted above regarding what the accuracy principle means in practice.

If organisations need to keep a record of a mistake, it should be identified clearly as a mistake. Records should clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. As a matter of good practice, organisations should keep a note of any challenges to the accuracy of personal data.

## 5. Fairness

Whether the Code sufficiently addresses standards of fairness within newsgathering practice, such as dealing fairly with those reported on and avoiding misrepresentation with respect to comment.

Processing personal data fairly, lawfully and transparently is one of the data protection principles. For more information about this principle, please see our Guide to UK GDPR – Lawfulness, fairness and transparency.

Unless the special purposes exemption applies (see above), organisations processing personal data for the purposes of journalism must comply with this principle.

It is likely to be unfair to process personal data in ways that people would not reasonably expect or if there is an unwarranted adverse effect on an individual. This general rule of thumb does not appear to be reflected in the current Standards Code clearly and we consider that its inclusion would be helpful.

Dealing with information lawfully and transparently are part and parcel of what it means to process information 'fairly'. The fact that they are part of one principle shows the close relationship between them. You may wish to consider reflecting this in the code.

Organisations must have a specific lawful basis before processing personal data – legitimate interests and consent are likely to be the most relevant to journalism. For more information, please see our Guide to UK GDPR Lawful basis for processing.

Organisations can rely on the 'legitimate interests' lawful basis when the processing is necessary to pursue legitimate interests which are not outweighed by any harm to an individual. The concept of 'fairness' is built into this balance.

There are high standards for consent under data protection law including that it should be opt-in; easy to understand; specific; granular; and easy

to refuse and to withdraw. Again, the idea of treating people fairly is readily apparent when considering consent.

Journalists will often wish to use 'special category' or 'criminal offence' data and need to note that there is extra protection afforded to sensitive personal data of this nature. For more information, please see the Guide to UK GDPR Special category data and Criminal offence data.

Organisations must generally provide clear privacy information to people when they collect their personal data but there are some exceptions when information is obtained from other sources. This is an important step to take in order to be transparent. Transparency is fundamentally linked to giving people more control and helping them to understand more clearly what is happening to their personal data. This is about treating people fairly too. For more information, please see Guide to UK GDPR – Right to be informed.

**6. Children**

Whether the Code is aligned with best practice with respect to informed consent and information gathering on matters affecting children.

Children need particular protection when organisations are processing their personal data because they may be less aware of the risks involved. For more information about data protection and the considerations that must take place with regard to children, please see our data protection guide to Children.

The key points of our guidance on children are summarised in the 'At a glance' sections. This includes legal requirements as well as good practice recommendations. We recommend that you consider these when reviewing this part of the Standards Code.

Organisations need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child. For more information, please see Guide to UK GDPR Lawful basis.

If organisations are relying on consent as the lawful basis for processing, when offering an online service directly to a child, only children aged 13 or over are able to provide their own consent.

For children under this age, organisations need to get consent from whoever holds parental responsibility.

You should also consider the Age Appropriate Design Code: a code of practice for online services. This came into force on 2 September 2020

with a 12 month transition period. Organisations must conform by 2 September 2021. Helpful information can be found in our associated Children's Code Hub.

It is a code of practice for providers of information society services. It applies to organisations when they provide online products or services (including apps, programs, websites, games or community environments, and connected toys or devices with or without a screen) that process personal data and are likely to be accessed by children in the UK. It is not only for services aimed at children.

The code sets out 15 flexible standards that help to protect children by ensuring that their best interests are the primary consideration when designing and developing online services. These standards should be helpful to you as you consider revising the Standards Code to reflect changes in the digital landscape and the impact on children.